The Ohio State Technology Law Journal

DIGITAL DATA AND THE FOURTH AMENDMENT: THE BIPARTISAN SOLUTION

RICHARD MCCUTCHEON[1]

ABSTRACT

The advent of digital technology created a slew of problems in applying the Fourth Amendment. In recent years, the Supreme Court has taken a more active approach in addressing the interaction between the Fourth Amendment and digital technologies. Two perspectives have emerged for justifying Fourth Amendment protections: one privacy-based and the other property-based.

The two approaches need not be mutually exclusive. This paper suggests a method to bridge the ideological divide in Fourth Amendment jurisprudence by combining the property and privacy perspectives into a unified test. This paper further suggests reforms that can be made to existing Fourth Amendment doctrine to return it to its ideological roots and facilitate the protection of digital data.

CONTENTS

---

[1] Student, The Ohio State University Moritz College of Law.

I. Introduction

Over the last decade, the Supreme Court has taken an interest in reexamining Fourth Amendment doctrine in a variety of different contexts as digital technology evolves.[2] The doctrine established in *United States v. Miller*[3] and *Smith v. Maryland*[4] during the late 1970s, known as the "third-party doctrine," has proven inadequate in protecting the privacy rights of Americans in the digital sphere.[5] The third-party doctrine states that content voluntarily disclosed to a third party for the third party's use does not receive Fourth Amendment protections.[6]

The concept of the third-party doctrine stems from an application of the precedent established in *Katz v. United States*, which states that Fourth Amendment protections only extend to circumstances where a person has a reasonable expectation of privacy.[7] The logic underpinning the *Smith* and *Miller* decisions is that information willingly shared with third parties carries no expectation of privacy.[8]

---

[2] *See, e.g.*, United States v. Jones, 565 U.S. 400 (2012); Riley v. California, 573 U.S. 373 (2014), Carpenter v. United States, 138 S. Ct. 2206 (2018).
[3] 425 U.S. 435 (1976).
[4] 442 U.S. 735 (1979).
[5] *See, e.g.*, Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. L. REV. 1441 (2017); Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985 (2016); Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 HARV. J.L. & TECH 1 (2017). In general, commentators have pointed out that the third-party doctrine, which is based on the technological paradigms of late 20th century American, has been overly broad and simplistic in its approach to digital technology.
[6] *See* Steven E. Henderson, *After* United States v. Jones, *After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 437-38 (2013).
[7] 389 U.S. 347, 360 (1967) (Harlan, J., concurring). Justice Harlan's concurrence outlines a two-prong test that has seen wide application since *Katz.* Fourth Amendment protections will be given if: (1) the individual had a subjective expectation of privacy and (2) that expectation of privacy was an expectation that society would deem reasonable. *Id.*
[8] *See Smith*, 442 U.S. 735; *Miller*, 425 U.S. 435.

Almost all modern communications require the use of third parties to function.[9] Every facet of American social and financial life conducted via the internet or over the phone including social media, banking, investment, dating, and retail is operated, managed, and recorded by third parties.[10] Yet, despite the massive amount of sensitive, personal information contained on these platforms, the Fourth Amendment affords those data essentially zero protection merely because they are held by third parties.[11]

The third-party doctrine, as applied to the internet and similar digital technologies, presents a major interpretive problem. Since internet architecture functions almost exclusively through the usage of third parties, vast amounts of data are often shared with third parties without the knowledge or explicit consent of the end user, which makes applying an analysis under the *Smith* and *Miller* framework practically unworkable.[12] Over the last decade, a majority of the Court[13] has gradually come to the conclusion that the current form of the third-party doctrine can no longer be reasonably maintained with regards to digital technology.[14] At the same time, however, the Court has not offered any substantial guidance as to what will replace the third-party doctrine, nor has the Court diminished its value as precedent.

In the most recent of these cases, *Carpenter v. United States*, the Court declined to apply the third-party doctrine in the context of Cell-Site

---

[9] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1089 (2002).
[10] *Id.*
[11] *See* Issacharoff & Wirshba, *supra* note 5, at 986.
[12] *See* Bellovin et al., *supra* note 5, at 3.
[13] Almost all Justices on the current Court disapprove of the third-party doctrine to some extent but differ as to the degree and the reasoning behind the disapproval. *See generally*, Carpenter v. United States, 138 S. Ct. 2206 (2018). The only Justices on the current Court whose opinion is not definitively known are Justices Kavanaugh and Barrett. *See id.* (Kavanaugh and Barrett were not on the Court at the time of *Carpenter* and have not yet issued an opinion on a major Fourth Amendment case).
[14] *See* Riley v. California, 573 U.S. 373, 400-01 (2014) (rejecting a "pre-digital" analogy test and the application of *Smith* to be of limited use when determining the government's accessibility to digital records). The Court acknowledged that "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" *Id.* at 403.

Location Information ("CSLI").[15] Cell phones are designed to continuously look for the nearest "cell-site"—essentially a radio antennae meant to connect the phone to wireless services—and produce CSLI when the phone connects to a cell-site, which timestamps the phone's geographic location in order to perform a variety of functions.[16] The Court described CSLI as a "distinct category of information" that was not covered by the third-party doctrine.[17]

Carpenter has caused a major debate and uncertainty in the current status of Fourth Amendment jurisprudence about the current status of the third-party doctrine. In addition, the decision has called into question the continued applicability of the *Katz v. United States*[18] reasonable expectation of privacy test. *Katz*'s reasonable expectation of privacy test provides the underlying framework for the third-party doctrine.[19] While Justice Roberts, writing for the majority in *Carpenter,* stated that the decision did not "disturb the application of *Smith* and *Miller*,"[20] the general consensus among academics, and even other members of the Court, is that the third-party doctrine is on "life support."[21] Consequently, the status of the third-party doctrine and the Fourth Amendment as it applies to digital information is uncertain.[22]

---

[15] *Carpenter*, 138 S. Ct. at 2210 (describing the grounds on which the Court distinguishes Cell-Site Location Information from the information in *Smith* and *Miller*).
[16] *Id.* at 2211-12.
[17] *Id.* at 2219. The Court, emphasizing how much technology has changed, further states that "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today." *Id.*
[18] 389 U.S. 347 (1967).
[19] *See, e.g.*, Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357 (2019); Trevor Burrus & James Knight, Katz *Nipped and* Katz *Cradled:* Carpenter *and the Evolving Fourth Amendment*, 2018 CATO SUP. CT. REV. 79 (2018); Sarah A. Mezera, Note, Carpenter*'s Legacy: Limiting the Scope of the Electronic Private Search Doctrine*, 117 MICH. L. REV. 1487 (2019); *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting).
[20] *Carpenter*, 138 S. Ct. at 2210.
[21] *Id.* at 2272 (Gorsuch, J., dissenting)*; see also id.* at 2247 (Alito, J., dissenting) (describing *Carpenter* as "fracturing two fundamental pillars of Fourth Amendment law" and "transform[ing] *Smith* and *Miller* into an unprincipled and unworkable doctrine."); Ohm, *supra* note 19; Michael Gentithes, *The End of* Miller*'s Time: How Sensitivity Can Categorize Third-Party Data After* Carpenter, 53 GA. L. REV. 1039 (2019).
[22] Academics have criticized the Court's lack of citation of legal scholarship in *Carpenter* that could potentially provide guidance for understanding its central holding. *See* Ohm, *supra* note 19, at 370. Ohm further notes that the decision in *Carpenter* resembles a version of a test

As Justice Sotomayor first noted in *United States v. Jones*, the Court needed to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[23] The Court has yet to come to an articulable and clear set of principles with regards to this "privacy regime" to supplement *Katz* in the realm of digital data. However, some academics, such as Georgetown Law Professor Paul Ohm, have speculated that *Carpenter* may completely supplant not only *Smith* and *Miller* but also *Katz* itself, and thus create an entirely new doctrine.[24] This new perspective on Fourth Amendment analysis, which Ohm characterizes as the "*Carpenter* test," creates a new three-prong evaluation which evaluates whether the category of information (1) has a deeply revealing nature; (2) possesses depth, breadth, and comprehensive reach; and (3) results from an inescapable and automatic form of data collection.[25] Even if *Carpenter* has not created a new test, the Court generally is trending toward being more inclusive of recognizing a Fourth Amendment interest in digital data and restricting the applicability of *Smith* and *Miller* to digital data.[26]

Others have noted that while the discussion regarding the fate of the third-party doctrine is ongoing among the majority,[27] the conservative

proposed by Susan Freiwald, but the Court does not indicate whether it was aware of the Freiwald's test when deciding *Carpenter*. *Id.* For an in-depth discussion on Freiwald's test, see Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011).

[23] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

[24] Ohm, *supra* note 19, at 378. Ohm gives several examples of what he speculates to be covered under this new test. Data likely to be covered under the *Carpenter* test includes information such as web browsing records and massive collections of telephone and banking records. *Id.* at 378-84. Ohm speculates that genetic information and medical information may be protected, but that their future is less certain with his proposed test. *Id.* at 378-85.

[25] *Id.* at 370. Ohm acknowledges there is likely to be significant disagreement about what factors *Carpenter* implies given the broad nature of the Court's opinion. *Id.* Consequently, it is important to consider Ohm's formulation as a test on a more conceptual level and as an articulation of potentially protectable principles rather than a definitive test.

[26] *Id.* at 358 (stating that *Carpenter* "has been heralded as a milestone for the protection of privacy in an age of rapidly changing technology").

[27] The current majority on this issue consists of Chief Justice Roberts, as well as Justices Sotomayor, Breyer, and Kagan. *See generally id.* Justice Kavanaugh has not articulated a clear position with regards to his perspective on Fourth Amendment jurisprudence either on the Supreme Court or in his previous position on the D.C. Circuit Court. *See* Orin Kerr, *Judge*

minority, comprised of Justices Thomas, Gorsuch, and Alito, has attempted to reinvigorate the "property-based regime" conceived prior to the *Katz* test.[28] These Justices consider whether the subject of the search is part of the individual's "person, house, papers, and effects"[29] to determine whether the subject enjoys Fourth Amendment protection.[30] While Justice Thomas and Justice Alito have denied that digital data held by third parties belongs to the individual whose information is contained on said data,[31] Justice Gorsuch has been more willing to recognize that one's digital data could be considered their "papers and effects."[32] Justice Gorsuch's willingness to break rank with his peers and extend Fourth Amendment protections to digital data is further indicia that the Court as a whole is increasingly considering digital data as a Fourth Amendment issue.

Kavanaugh on the Fourth Amendment, SCOTUSBLOG (July 20, 2018, 6:16 PM), https://www.scotusblog.com/2018/07/judge-kavanaugh-on-the-fourth-amendment/ [https://perma.cc/RCT8-FEBR]. Kerr warns against reading too much into Justice Kavanaugh's prior rulings given his "modest" record. Nonetheless, there is some indication that Justice Kavanaugh may harbor sympathies for both the majority and conservative minority regarding this issue. *See* United States v. Jones, 625 F.3d 769-71 (D.C. Cir. 2010) (order denying rehearing) (Kavanaugh, J., dissenting). Justice Barrett's opinion is also not yet known.

[28] Carpenter v. United States, 138 S. Ct. 2206, 2235 (2018) (Thomas, J. dissenting) (stating that the "Fourth Amendment guarantees individuals a right to be secure from unreasonable searches of *'their* persons, houses, papers and effects'"); *Id.* at 2240 (Alito, J., dissenting) (stating "the organizing constitutional idea of the founding era . . . was property."; *Id.* at 2267-68 (Gorsuch, J., dissenting) (explaining that "the traditional approach asked if a house, paper or effect was *yours* under law. No more was needed to trigger the Fourth Amendment"). Justice Thomas explicitly disapproved of the *Katz* reasonable expectation of privacy test, calling it a "failed experiment." *Id.* at 2246 (Thomas, J., dissenting).

[29] U.S. CONST. amend. IV.

[30] *Carpenter*, 138 S. Ct. 2206, 2235 (Thomas, J., dissenting); *id.* at 2267-68 (Gorsuch, J., dissenting); *id.* at 2257 (Alito, J., dissenting).

[31] *Id.* at 2235 (Thomas, J., dissenting) ("[The defendant] did not create the records, he d[id] not maintain them, and he cannot destroy them. Neither the terms of his contracts nor any provision of law makes the records his. The records belong to [the third party.]"); *id.* at 2257 (Alito, J., dissenting) (explaining that "[there is] no right to demand the [third party] destroy the records, no right to prevent the providers from destroying the records . . . to modify the records . . . [and] no meaningful control over the [records] which are [managed] by [the third party.]").

[32] *Id.* at 2268-69 (Gorsuch, J., dissenting) (explaining that the mere fact that a third party has "access to or possession of your papers and effects does not necessarily limit your interest in them" and further describing how the concept of bailment could potentially be applied to digital data).

As Justice Gorsuch acknowledges, the property-based regime does not extinguish the *Katz* privacy regime, and the two doctrines can exist concurrently.[33] The *Katz* privacy regime does not abridge the expressly enumerated rights found in the Fourth Amendment itself, and the property-based regime does not preclude a *Katz* analysis from being conducted. Consequently, a bipartisan doctrinal answer may be possible in the wake of *Carpenter*, as the current Court seems to be protective of digital privacy rights and trending toward a more inclusive understanding of the Fourth Amendment from both a privacy and property-based perspective.

This Note discusses the two types of philosophical underpinnings of Fourth Amendment jurisprudence: the property-based perspective and the *Katz* privacy perspective. In Part II, the Note will explore the history and development of Fourth Amendment jurisprudence to distill the essence of Fourth Amendment jurisprudence into a set of articulable principles. Part III will explore the development of the current precedent in detail and illustrate how *Smith* and *Miller* have decoupled Fourth Amendment jurisprudence from both the privacy and property perspective's philosophical interests. Part IV bridges the gap between the property-based regime and the privacy regime to create a bipartisan, technology inclusive doctrine that favors the private individual to govern digital technology moving forward. Part V concludes.

II. Legal History

Privacy and property rights have always been essential principles underpinning Fourth Amendment jurisprudence.[34] For a time, however, the Fourth Amendment was thought to protect only tangible property seized from a constitutionally protected area, such as one's person or domicile.[35] With the rise and prominence of electronic surveillance

---

[33] *Id.* at 2268 (Gorsuch, J., dissenting) (quoting Byrd v. United States, 138 S. Ct. 1518 (2018) ("*Katz* supplements, rather than displaces 'the traditional property-based understanding of the Fourth Amendment'")).

[34] *See, e.g.*, *ex parte* Jackson, 96 U.S. 727, 733 (1877) (describing the importance of the "secrecy of letters"); Katz v. United States, 389 U.S. 347, 352-53 (1967) (stating that the Fourth Amendment was thought to limit seizures of only tangible property).

[35] *See* Olmstead v. United States, 277 U.S. 438, 466 (holding that only a physical invasion of the home or seizure of tangible material effects enjoyed Fourth Amendment protection). *But*

midway through the Twentieth Century, the Court began to reassess its position and the foundation of the Fourth Amendment in property principles.[36] By the latter half of the Twentieth Century, the privacy perspective of the Fourth Amendment began to dominate the jurisprudence, culminating with *Katz* explicitly rebuking the exclusively property-based perspective.[37] However, the implementation of an unfettered privacy perspective in *Katz* has led to strange results and doctrinal issues such as the third-party doctrine established in *Smith* and *Miller* that undermine the intention of the Fourth Amendment's underlying principles.

A. *Ex Parte Jackson*: Where All Roads Lead Back To

Ex parte Jackson revolves around a relatively simple set of facts. Despite its simplicity, *Jackson* is exceptionally valuable for understanding the principles underpinning the vast majority of Fourth Amendment jurisprudence. *Jackson* provides an exemplary case study in how the Court treats different categories of information.

In 1877, A. Orlando Jackson had been convicted for illegally circulating a flier concerning a lottery through the U.S. Postal Service.[38] Congress had previously declared in 1868 that attempting to send mail concerning lotteries was unlawful.[39] Despite this, Jackson attempted to send his letter without any attempt to hide its contents via an envelope or

---

see, JOHN LOCKE, TWO TREATISES OF GOVERNMENT 287-88 (P. Laslett, ed. 2002) (describing a theory of property that creates a property interest in not only tangible objects, but also in labor); JACK RAKOVE, REVOLUTIONARIES: A NEW HISTORY OF THE INVENTION OF AMERICA 78 (2010) (explaining that the Lockean idea of property did not only encompass tangible objects, but also the rights to acquire tangible objects as the result of one's labor).

[36] *See, e.g.*, Wong Sun v. United States, 371 U.S. 471 (1962) (holding that intangible communications could be improperly seized and were subject to the exclusionary rule).

[37] *See Katz*, 389 U.S. at 353 ("But the premise that property interests control the right of the Government to search and seize has been discredited"). The Court has repeatedly stated that the Fourth Amendment does not only extend to the seizure of tangible items. *Id.*

[38] *Jackson*, 96 U.S. at 728.

[39] *Id.* at 730.

otherwise.[40] Jackson appealed his conviction as unconstitutional on First Amendment grounds.[41] The appeal was unsuccessful.[42]

While the Court upheld Congress' right to regulate mail, it also articulated a clear standard for what types of personal property were protected under the Fourth Amendment and how inspection should be handled.[43] The Court widened the scope of the Fourth Amendment to protect items outside of a person's home, such as their papers and effects, but only under certain circumstances.[44] To this effect, the Court stated:

> [A] distinction is to be made . . . between what is intended to be kept free from inspection, such as letters, and sealed packages . . . and what is open to inspection, such as . . . [mail] purposely left in a condition to be examined. [Mail] of this kind in the mail are fully guarded . . . except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.[45]

---

[40] *Id.* at 737. The Court noted that the circular was "left open for examination." *Id.* The Court notes in the syllabus that the mail was "enclosed in an envelope," yet from the language of the court and holding of the case, it can be inferred that the circular was still visible despite being in an envelope. *See id.* at 728. The Court does not describe how or why the circular was visible to the postal inspectors, however.

[41] *Id.* at 730. Jackson's original petition did not contemplate a Fourth Amendment remedy, but the Court nonetheless analyzed the seizure of his mail under the Fourth Amendment, along with his First Amendment claim.

[42] *Id.* at 737. The Court denied the First Amendment petition on the grounds that Congress had the enumerated authority to regulate the mail and had the right to "refuse its facilities for the distribution of matter deemed injurious to the public morals." *Id.* at 736.

[43] *Id.* at 733. The standard originating in *Jackson* is often termed the "content/envelope" or "content/non-content" distinction by academics. Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2112 (2009). This distinction is not only present in Fourth Amendment jurisprudence, but also statutory law regarding electronic surveillance. *Id.*; *see also* Bellovin et al., *supra* note 5, at 12. In the context of internet and digital technologies, however, the distinction has repeatedly come under criticism as being inapplicable and creating impractical, unworkable doctrines. *See* Bellovin et al., *supra* note 5, at 20-22.

[44] Burrus & Knight, *supra* note 19, at 82 (describing how *Jackson* did not impose a location requirement on whether a person's papers or effects are covered by the Fourth Amendment).

[45] *Jackson*, 96 U.S. at 733. The "outward form and weight" of the letter forms the basis of what is traditionally considered to be "non-content," whereas the letter itself is considered "content." *See* Tokson, *supra* note 43, at 2112. The Court highlights the importance that the

The main principle expressed by the Court is clear: Unless the mail was sent in a manner that plainly revealed its contents, it will generally enjoy the protection of the Fourth Amendment as a person's "papers and effects" except as to what is plainly visible from its "outward form and weight."[46]

The principle intuitively makes sense. Postal inspectors and the police should not willfully blind themselves to what is plainly visible. For physical mail to function, one must read the writing on the envelope to know where it is headed, how much a package weighs, and what it looks like. Subjecting such information to Fourth Amendment scrutiny would make running the postal service without a constitutional violation all but impossible.

Another principle not explicitly stated in the opinion, but which can be felt underlying its reasoning, is the expectation of privacy that would be further developed and formally recognized in *Katz*.[47] The same line of thought would later be used to develop the third-party doctrine in *Miller* and *Smith*.[48] The sender of the letter that knows certain information (i.e. its exterior) will be seen by the government as a practical matter—the sender voluntarily chose to share that information.[49] The sender

---

"outward form and weight" is a property of the evidence that is "seen by everyone, and is in its nature conclusive." *Jackson*, 96 U.S. at 736.

[46] *Jackson*, 96 U.S. at 736. The Court clarifies that "no difficulty arises, and no principle is violated, in excluding the prohibited items or refusing to forward them" in circumstances where "the object is exposed, and shows unmistakably that it is prohibited." *Id.*

[47] The Court in *Jackson* notes that people have a constitutional right in papers "closed against inspection, wherever they may be" and that Congress may not "invade the secrecy of letters." *Id.* at 733. The significance the Court places on whether the person has actively concealed their papers from inspection implies an expectation of privacy that otherwise is not contained in the literal language of the Fourth Amendment, which makes no such distinction between concealment and public display of papers. *See also* Katz v. United States, 389 U.S. 347 (1967).

[48] *See* Burrus & Knight, *supra* note 19, at 81. Similar to how *Jackson* does not afford Fourth Amendment protections to information visible to a government agent (i.e., the postage officer), *Smith* and *Miller* stand for the contention that information turned over to a third party for the third party's use carries no Fourth Amendment protections. Information that a third party is expected to view or use does not enjoy privacy protections. *See id.*

[49] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (describing the subjecting reasonableness requirement to enjoy Fourth Amendment protections).

understands and consents to the fact that the information on the envelope will be read and its container scrutinized but considers the contents of the letter itself to be private. Hence, the contents are protected under the Fourth Amendment. In the words of the Court, the letter's "contents" are to be treated as "papers subject to search in one's own household."[50]

B. *Olmstead*, *Wong Sun*, and *Berger*: Protecting "Intangible" Communications

While *Jackson* protected physical property—such as letters—prior to the 1967 *Berger v. State of N.Y.*[51] case, the Court had not recognized similar protections for communications via telephone.[52] The Court ruled in *Olmstead v. United States* that wiretapping did not amount to a search or seizure under the Fourth Amendment.[53] The Court would not acknowledge the government's seizure of communications as constitutionally protected until *Wong Sun*[54] and would not apply it in a surveillance context until *Berger*.[55]

1. *Olmstead v. United States*: An Inspirational Dissent

The Court's decision in *Olmstead* rejecting any constitutional protection against wiretapping came from a narrow interpretation of the holding in *Jackson*: wiretapping a telephone neither seized any tangible effects or papers nor invaded a "constitutionally protected area" (e.g. residence or place of business).[56] Telephone wires extended beyond the home, and nonphysical communications—which were not papers or effects—intercepted via a device placed outside the home of suspects were not protected by the Fourth Amendment.[57]

---

[50] *Jackson*, 96 U.S. at 733.
[51] 388 U.S. 41 (1967).
[52] *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).
[53] *Id.*
[54] Wong Sun v. United States, 371 U.S. 471, 485 (1963).
[55] *Berger*, 388 U.S. at 63.
[56] *Olmstead*, 277 U.S. at 466. Although all communications have some physical properties to them and potentially can be manifested in a permanent, physical form, the Court did not consider verbal communications sufficiently tangible to constitute a person's "effects." *See id.*
[57] *Id.* The wiretaps used in *Olmstead* were placed in the telephone wires that ran throughout the streets near the defendant's houses. *Id.* at 456-57.

In his now-famous dissent, which later informed a slew of decisions, including *Berger* and *Carpenter*,[58] Justice Brandeis expressed his concern over the "[s]ubtler and more far-reaching methods of invading privacy" available to the government that were "more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[59] Disputing the Court's interpretation of *Jackson*, Brandeis argued that there was no legal difference between a private telephone conversation and a sealed letter.[60] The invasion of privacy was far greater by wiretapping than by tampering with the mail, as it implicated not only more sensitive information but also multiple individuals.[61]

Through a wiretap, the government could obtain a much greater volume of confidential and private information about an individual than by mail. Brandeis described traditional means of espionage as "but puny instruments of tyranny and oppression when compared with wire tapping."[62] Speaking on the intentions and principles of the Framers, Brandeis noted that the Fourth Amendment protects against unjustifiable intrusion by the government regardless of the means.[63] Whether the information seized was "tangible" or not had no bearing.

Brandeis' broader interpretation of the Fourth Amendment eventually became the backbone underlying *Wong Sun v. United States*, *Berger*, and, finally, *Katz*, which directly overturned *Olmstead* and created an entirely new standard under which all Fourth Amendment cases are now evaluated.[64]

---

[58] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (quoting *Olmstead*, 277 U.S. at 473-74 (Brandeis, J., dissenting)). The Court in *Carpenter* acknowledges the profound influence Brandeis' dissent in *Olmstead* has had on shaping Fourth Amendment discourse. *Id.*
[59] *Olmstead*, 277 U.S. at 473-74 (Brandeis, J., dissenting).
[60] *Id.* Brandeis goes on further to note that "in the application of a Constitution, our contemplation cannot be only of what has been, but what may be." *Id.*
[61] *Id.* at 475-76. Brandeis articulates that the purpose behind the Fourth Amendment is not merely meant as a defense against the invasion of physical property, but also an "indefeasible right of personal security, personal liberty, and private property." *Id.*
[62] *Id.* at 476. Brandeis' concerns not only reflect his reservations about the wiretap specifically, but of all future surveillance technology developments. *See id.*
[63] *Id.* at 478.
[64] *See generally* Katz v. United States, 389 U.S. 347 (1967).

2. *Wong Sun v. United States*: The Unexpected Surveillance Case

Wong Sun v. United States, a case completely unrelated to wiretapping, had a massive impact in redefining the Court's approach to the Fourth Amendment and, by extension, government surveillance.[65] Previously, in cases such as *Silverman v. United States*[66] and *Goldman v. United States*,[67] the Court had declined to upend the precedent established by *Olmstead* and narrowly construed the Fourth Amendment to tangible objects.[68] Neither *Goldman* nor *Silverman* affected the central holding of *Olmstead*, but *Silverman* managed to slightly shift the conversation. *Silverman* stood for the general idea that a physical intrusion into a "constitutional protected area" was an unwarranted search, and it prohibited the use of the observed communications, but it did not focus on whether the taking of the communications was a "seizure."[69] The Court's finding in *Silverman* was nonetheless a small but significant departure from *Olmstead*, as the exclusionary rule traditionally barred only physical, tangible materials obtained as a result of a lawful invasion.[70]

---

[65] *See generally* 371 U.S. 471 (1963) (holding that communication is protected by the Fourth Amendment).
[66] *See* 365 U.S. 505 (1961) (holding that a "spike mike" attached to the heating duct of defendant's home was a search).
[67] *See* 316 U.S. 129 (1942) (holding that a detectaphone placed in a room adjoining the office of defendant was not a search under the Fourth Amendment and explicitly declining to overturn *Olmstead*).
[68] The articulable distinction between *Silverman* and *Goldman* was that although both involved government surveillance efforts, only in *Silverman* did the device physically enter the home, and therefore was prohibited. *See Silverman*, 365 U.S. 505. By contrast, *Goldman* involved a device placed outside of the defendant's residence, and therefore was considered permissible. *See Goldman*, 316 U.S. 129.
[69] *See Silverman*, 365 U.S. at 512. (Stewart, J., writes "it is based upon the reality of an actual intrusion into a constitutionally protected area."). *Silverman* reflects the first time that the Court has decided to exclude oral statements observed via an invalid search.
[70] *See Wong Sun*, 371 U.S. at 485 (discussing the impact of *Silverman* on the Court's holding and the lack of meaningful distinction between verbal and "physical" evidence for the purposes of the exclusionary rule). The Court in *Silverman* did not attempt to reconcile the logical contradiction of barring Fourth Amendment protections to oral communications (i.e., there were not objects that could be improperly seized) yet still preventing them from being introduced in Court when obtained in an improper search.

With *Wong Sun,* the paradigm would shift, and the Fourth Amendment would protect against the seizure of verbal statements by "eavesdropping" law enforcement.[71] While semantically the term "eavesdropping" may seem to imply the use of surveillance technology, the facts of *Wong Sun* involve no devices other than the human ear.[72] Federal narcotics agents had unlawfully entered the residence of James Wah Toy under the suspicion that he had been selling heroin.[73] Upon entering Toy's home, the agents detained and interrogated Toy, who stated that, while he did not sell heroin, he knew a man named Johnny who did.[74] Agents found a man by the name of Johnny Yee, who surrendered a small amount of heroin and stated that he got it from another man, Wong Sun.[75]

The Court threw out Toy's statements under the doctrine of fruit of the poisonous tree.[76] In the Court's view, the Fourth Amendment safeguarded "verbal statements as well as the more traditional seizure of 'papers and effects.'"[77] While still in the context of an unlawful physical intrusion by law enforcement, the formal recognition of speech as the equivalent of "papers and effects" changed Fourth Amendment jurisprudence to include non-tangible information. Brandeis, for the time being, had been vindicated.

---

[71] *Id*. at 486.
[72] *Id.* at 474.
[73] *Id.* Federal agents had broken into Toy's laundry service (where he also lived) following an exchange wherein Toy slammed the door after an agent identified himself as a narcotics officer and fled from the business area of the laundromat to his living quarters. *Id.* In response, the agents broke down the door to pursue Toy. *Id*. The agents did not have a warrant when they entered Toy's residence. *Id.*
[74] *Id.* The amount of heroin surrendered was less than one ounce. *Id.*
[75] *Id.* at 475. Through a convoluted series of events, Johnny Yee identified Wong Sun by his nickname, "Sea Dog" and the narcotics agents had to return to Toy to interrogate him a second time to find out that "Sea Dog" was Wong Sun. *Id.*
[76] *Id.* at 485. The fruit of the poisonous tree prohibits the introduction of illegally obtained evidence. *See* Nardone v. United States, 308 U.S. 338 (1939) (coining the phrase "fruit of the poisonous tree").
[77] *Wong Sun*, 371 U.S. at 485.The Court logically inferred this distinction from *Silverman*, stating that verbal and physical evidence were both "fruits" of an invalid search. *Id.*

3. *Berger v. New York*: Overturning *Olmstead*

Berger took the principles from *Wong Sun* and applied them to the context of electronic surveillance.[78] Specifically, the Court ruled that statutes authorizing eavesdropping had to be construed to meet the Fourth Amendment's warrant requirement.[79] Failure to adhere to the warrant requirement would bar the "fruit" or communications obtained by wiretap or bug.[80] Echoing Brandeis's dissent from *Olmstead*, the Court noted that "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices."[81]

The holding of *Berger* overturned *Olmstead sub silentio*.[82] A wiretap capturing conversations, even if physically affixed outside of a constitutionally protected area, constituted a search within the meaning of the Fourth Amendment.[83] Under the Court's construction, a wiretap *did* invade the privacy of one's home.[84]

But what about wiretaps or other surveillance devices that record people outside of their homes? For better or worse, the issue had still been couched in the "constitutionally protected area" language established in *Olmstead*.[85] Since the Court in *Berger* framed the issue in terms of surveillance conducted on a person's residence or place of business, the

---

[78] *See* Berger v. N.Y., 388 U.S. 41 (1966). Berger specifically concerned a New York statute authorizing law enforcement to eavesdrop via electronic surveillance with "reasonable grounds." *Id.* at 51. The Court noted that "the law, though jealous of individual privacy, has not kept pace with [advances in surveillance technology.]" *Id.* at 49.

[79] *Id.* at 63. The Court additionally provided a common law basis against eavesdropping generally, noting that it was historically recognized as a nuisance. *Id.* at 45. The Court criticized the state as allowing officers "a roving commission to 'seize' any and all conversations." *Id.* at 59.

[80] *Id.* at 63.

[81] *Id.*

[82] *Id.* at 64 (Douglas, J., concurring). The Court at no point in the majority opinion directly states that it is overturning *Olmstead* (in other words, it overturned *Olmstead sub silentio*), but Justice Douglas immediately highlights this fact in his concurrence. *Id.*

[83] *Id.* at 51 (majority opinion). Notably, the Court considered a wiretap, even if physically affixed outside the home or office, a "trespassory invasion." *Id.* at 64.

[84] *Id.* at 51.

[85] Even though the Court had gone to great lengths to establish the "basic right to privacy" in *Berger*, that privacy only extended to "one's home" and did not encompass other interactions outside the home (or constitutionally protected areas), no matter how sensitive or "private" they might be. *See id.* at 63.

question of what Fourth Amendment protections existed for a person being surveilled outside the home during his or her everyday life remained.

That question would be answered in *Katz*, which would completely redefine the standards under which the Fourth Amendment would be governed.

C. *Katz* Changes Everything

Charles Katz was indicted for gambling by placing wager information using a public telephone booth.[86] At his trial, the Government introduced evidence collected by FBI agents via a wiretap placed on the booth, and Katz was convicted.[87] Katz appealed, arguing that the wiretap violated his Fourth Amendment rights, and the Court agreed.[88]

The Court in *Katz* stated that "the Fourth Amendment protects people, not places."[89] Citing *Jackson*, among other things, the Court noted that what a person intended to keep private, even in areas accessible to the public, may be constitutionally protected.[90] Conversely, what is knowingly exposed to the public, even when within a private home or office, does not enjoy Fourth Amendment protections.[91] The latter principle would become part of the foundation of the third-party doctrine in *Smith* and *Miller*.[92]

---

[86] Katz v. United States, 389 U.S. 347, 348 (1967).
[87] *Id.*
[88] *Id.* The Court specifically rejected Katz' formulation of the issue, which he based on whether a telephone booth was a constitutionally protected area, stating "the correct solution of Fourth Amendment problems is not necessarily promoted by the incantation of the phrase 'constitutionally protected area.'" *Id.* at 350.
[89] *Id.* at 351.
[90] *Id.* ("[W]hat [the individual] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").
[91] *Id.* For example, a person has no privacy interest in acts that they perform that are visible from an unobstructed window in his or her home, even it is technically within a "private" location. *See id.*
[92] Smith v. Maryland, 442 U.S. 735, 743-44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

While *Berger* retained most of the legal framework of protection from invasion of constitutionally protected areas from *Olmstead*, the Court in *Katz* functionally abandoned this idea.[93] Explicitly overturning *Olmstead*, the Court concluded that Fourth Amendment protections do not turn on "the presence or absence of physical intrusion into any given enclosure."[94] Instead, the new consideration for whether the Fourth Amendment applied would be centered around a more nebulous conceptualization of privacy,[95] which was not meaningfully analyzed in the Court's ruling.[96]

While the rebuke of *Olmstead* was significant, the most important and enduring component of *Katz* did not come from the majority's opinion but rather from Justice Harlan's concurrence.[97] The explanation of principles in Harlan's concurrence would lead to the creation of the reasonable expectation of privacy test.[98] The test featured two prongs to establish Fourth Amendment protection: (1) that a person exhibited an actual, subjective expectation of privacy, and (2) that the expectation is one that society deems "reasonable."[99]

---

[93] Peter Winn, Katz *and the Origins of the Reasonable Expectation of Privacy Test*, 40 MCGEORGE L. REV. 1, 6 (2009). The Court noted the Fourth Amendment "protected individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all." *Katz*, 389 U.S. at 350.

[94] *Katz*, 389 U.S. at 353.

[95] The majority opinion in *Katz* provides a major shift in perspective on how Fourth Amendment jurisprudence should be handled from the more traditionalist property-based perspective to a privacy-based perspective, which has a more indefinite and broader approach than the previously used property-based perspective. *See generally id.* Even though *Katz* shifts the focus, it is important to note that *Katz* was not intended to diminish the Fourth Amendment's scope of protection, not constrain the Fourth Amendment to *solely* a privacy perspective. *See id.* at 350 (stating that the Fourth Amendment does not protect a general right to privacy and is not limited to merely privacy rights).

[96] *See generally id.* (Justice Stewart, writing for the majority, does not provide details for what a reasonable expectation of privacy is).

[97] Winn, *supra* note 93, at 7. It is widely acknowledged that Justice Harlan's concurrence has overridden the majority opinion in terms of relevance. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33 (2001) (describing Justice Harlan's "oft-quoted concurrence"); Minnesota v. Carter, 525 U.S. 83, 97 (1998) (stating that the *Katz* test refers exclusively to Justice Harlan's concurrence) (Scalia, J., concurring).

[98] Winn, *supra* note 93.

[99] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

The principles expressed under *Katz* harken back to the concepts first espoused in *Jackson.* Much like how a person cannot have a reasonable expectation that writing on an envelope's exterior would go unread, "conversations in the open would not be protected against being overheard."[100] Through *Katz*, the principles and expectations set forth in *Jackson* were finally incorporated for communication and expression. But what happens when the communications are monitored or recorded by non-government third parties? *Katz* clearly establishes that communication is equivalent to one's papers and effects, both of which require a warrant to be seized.[101] But *Katz* says nothing about communications retained by third parties.

Surveillance statutes following *Katz*, such as Title III of the 1968 Omnibus Crime Control and Safe Streets Act[102] (hereinafter "Wiretap Act"), provided strong protections for the "contents" of any wire, electronic, or oral communication intercepted by government devices.[103] Contents were defined as "any information concerning the substance, purport, or meaning" of that communication.[104] The Wiretap Act only protected communication being "intercepted" by government devices, which provided no barrier to prevent the government from obtaining information held by third parties.[105]

D. *Miller* and *Smith*: Third-Party Doctrine Muddies the Water

The beginnings of a doctrine that would perplex and dismay modern privacy academics started in 1976 with *Miller* and were later refined in

---

[100] *Id.* The language used here can be seen as analogous to the "outward form and weight" language employed in *Jackson. See ex parte* Jackson, 96 U.S. 727, 733 (1877).
[101] *See* 389 U.S. at 358-59.
[102] Omnibus Crime Control and Safe Streets Act, PUB L. NO. 90-351, §§2510-2520, 82 Stat. 197, 211-25 (1968) (codified as amended at 18 U.S.C §§ 2510-2530 (2012)).
[103] 18 U.S.C § 2510(8) (original definition of "contents" from the Wiretap Act).
[104] *Id.* Records maintained by third parties regarding phone calls were not considered to be "content" for the purposes of this definition. *Id.*
[105] *Id.* The distinction between "intercepted" and "held" in this case refers to the transitory nature of the information. Under the Wiretap Act, the government was restrained from actively listening to an ongoing conversation. *See id.* However, the government was not restricted from seizing a transcript of a conversation being held in storage by a third party under the Wiretap Act. *See id.*

Smith.[106] Other cases had previously addressed disclosures to third parties, such as *Lopez v. United States*[107] and *Hoffa v. United States*,[108] but they did so under the pre-*Katz* Fourth Amendment framework.

Three years prior to *Miller*, the Court considered the issue in passing. In *Couch v. United States*, the Court ruled that financial information disclosed to an accountant—which would be provided to the IRS—carried no reasonable expectation of privacy, but this issue was primarily considered in the context of the Fifth Amendment and property ownership.[109] *Miller*, however, would more fully analyze the issue in the context of the *Katz* standard expressed under the Fourth Amendment.[110] Three years after *Miller*, *Smith* would drastically expand the surveillance power of the government by expanding the scope of the third-party doctrine.[111]

1. *United States v. Miller*: The Humble Beginnings of the Third-Party Doctrine

Miller involved defendant Mitchell Miller, who was convicted of operating a whiskey distillery without a license.[112] During the investigation headed by the Treasury Department's Alcohol, Tobacco, and Firearms Bureau, agents served defective subpoenas to obtain

---

[106] *Accord* Bellovin et al., *supra* note 5, at 5; *see also* Tokson, *supra* note 43, at 2106 (noting that third-party doctrine has been a contentious point of discussion among academics).
[107] 373 U.S. 427 (1963) (regarding the attempted bribe of a tax official). The Court distinguished *Lopez* from *Wong Sun*, which was decided in the same year, on the grounds that the defendant in *Lopez* had consented to the official being in his home. *Id.* at 438.
[108] 385 U.S. 293 (1966) (regarding verbal disclosures made to a government informant in a hotel room). The Court noted that a hotel room can be the subject of Fourth Amendment protection as much as a home or office but ruled that Hoffa did not have any privacy expectation with regards to the communications he gave to a government informant he willingly invited into that space. *Id.* at 301, 303.
[109] 409 U.S. 322 (1973). Although primarily engaging in a Fifth Amendment analysis, the Court conducted a reasonable expectation of privacy test, finding "there can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return." *Id.* at 335.
[110] *See* Rebecca Lipman, Note, *Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age*, 8 HARV. L. & POL'Y REV. 471, 474 (2014).
[111] *See* Smith v. Maryland, 442 U.S. 735, 744-45 (1979).
[112] United States v. Miller, 425 U.S. 435, 436 (1976).

microfilm records of defendant's banking information.[113] Miller asserted a Fourth Amendment defense, arguing that his private papers had been improperly seized and therefore could not be used as evidence against him.[114]

The Court did not agree.[115] Miller's banking information was not considered to be "private papers" and did not require a warrant to be seized.[116] The fact that the subpoenas were defective proved to be irrelevant.[117]

Using the reasonable expectation of privacy standard expressed in *Katz*, as well as the principles first conceived in *Jackson*, the Court ruled that Miller had no reasonable expectation of privacy in the contents of financial statements and deposit slips.[118] The Court emphasized that banking documents seized were not confidential communications but instead business instruments used for commercial transactions.[119] Further, the documents were based on information voluntarily conveyed to the bank and exposed to its employees in the ordinary course of business.[120] The depositor "takes the risk" that the information could be disclosed to the government.[121]

The important takeaway from *Miller*, which would later be used in *Carpenter,* is that information tendered to a third party would not be protected if the information conveyed was voluntarily given, non-sensitive, used in the ordinary course of business, and exposed to

---

[113] *Id.* at 437-38.
[114] *Id.* at 438-39.
[115] *Id.* at 440.
[116] *Id.*
[117] *Id.* at 441. Since Miller had no Fourth Amendment protections and the bank had voluntarily disclosed Miller's information, there was no requirement to subpoena the bank for records. *Id.* at 443.
[118] *Id.* at 442.
[119] *Id.* The bank itself disputed this characterization and indicated that the customer's account information was considered by its customers to be confidential, which Justice Brennan highlighted in his dissent. *Id.* at 449 (Brennan, J., dissenting).
[120] *Id.*
[121] *Id.* at 443.

employees.[122] This specific, more concrete standard would erode as technology and the third-party doctrine developed, starting with *Smith.*[123]

2. *Smith v. Maryland*: The Broadening of the Third-Party Doctrine

While *Miller* dealt primarily with a search in the traditional context of seizing physical assets from a third party, *Smith* revolved around search and seizure as it related to government-surveillance. In March of 1976, a Baltimore resident by the name of Patricia McDonough was robbed.[124] After the robbery, McDonough received a series of threatening calls from an unknown man, who identified himself as the robber.[125] McDonough spoke to police who, without a warrant, requested that the telephone company install a pen register, which is a device that monitors the numbers dialed by telephone users.[126] From this installation, the police discovered that Michael Lee Smith, a person who was already under suspicion, had placed a call to McDonough's house.[127] Using this discovery along with other evidence, the police arrested Smith, who was then identified by McDonough as the robber.[128] At trial, Smith motioned to have "all fruits derived from the pen register" suppressed.[129]

The Court denied Smith's motion and stated that installation of the pen register was not a search.[130] In distinguishing *Smith* from *Katz*, the Court stated that a pen register did not record the *contents* of communications,[131] an interpretative distinction originally employed by

---

[122] Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1928 (2017) [hereinafter "*If These Walls Could Talk"*].
[123] *Id.* at 1929.
[124] Smith v. Maryland, 442 U.S. 735, 737 (1979).
[125] *Id.*
[126] *Id.* A pen register will record where a phone places a call and the time the call is made. *Id.* at 736 n.1.
[127] *Id.*
[128] *Id.* Smith also happened to have a phone book containing McDonough's number circled in it. *Id.*
[129] *Id.* at 737.
[130] *Id.* at 745-46.
[131] *Id.* at 741.

the Court in *United States v. New York Telephone Co.*, which concerned the required procedures of the 1968 Wiretap Act and did not directly reach a Fourth Amendment question.[132] Consequently, *Smith* represented the first time that the constitutionality of the pen register was directly challenged.

In another first, the Court explicitly used Justice Harlan's test expressed in *Katz* and determined that Smith had no reasonable expectation of privacy in the phone numbers he dialed.[133] The Court argued that Smith must have realized that he "conveyed" the numbers he dialed to the telephone company.[134] Crucial to the Court's reasoning in this instance was the fact that telephone companies provided resources to customers that indicated numbering information was recorded, such as long-distance call bills, telephone directories, and phone books, all of which allowed them to infer that call information was being recorded.[135]

Citing *Miller*, the Court noted that Smith had assumed the risk of exposing his dialing information to the telephone company and analogized telephone company's automated recording services as the metaphorical equivalent of a telephone operator that would take and redirect calls.[136] The shift away from the original principles of *Miller* and *Jackson* was subtle but had a pronounced effect. By putting forth the idea that an automated register was the equivalent of a telephone operator, the Court whittled away at one of the factors that underpinned

---

[132] 434 U.S. 159, 165-67 (1977). Contents of communications enjoyed the full protection of the Fourth Amendment. *See id.* Third-party records obtained in connection with those communications (also known as "non-content") did not. *See id.* at 168.

[133] *Smith*, 442 U.S. at 745. There is no indication that Smith actually knew that he had conveyed his phone dialing information to the telephone company. *See id* at 742.

[134] *Id.*

[135] *Id.* at 742-43. Justice Marshall expressed significant skepticism regarding this particular point, stating "I do not [assume] that individuals 'typically know' that a phone company monitors calls for internal reasons." *Id.* at 749 (Marshall, J., dissenting). Further, Justice Marshall challenged the notion that even if an individual was aware, he or she did not expect the call information to be handed out to the public at large or the government. *Id.*

[136] *Id.* at 744-45 (majority opinion). The Court did not address the issue of whether communications given a telephone operator or subsequent records of a conversation kept by a telephone operator were subject to Fourth Amendment protections. *See generally id.*

the expectation of privacy: exposure to other people in the ordinary course of business.[137]

The subtle change in meaning of the word "voluntary" as expressed under *Miller* when compared to how "voluntary" is used in *Smith* is also worth noting. In *Miller*, and other related cases prior to *Miller*, the information in question was knowingly and explicitly turned over to the third-party recipient.[138] In *Smith*, the phone records were conveyed neither by the explicit intention of Smith, nor is it likely that he knew the phone company retained his dialing history.[139]

Smith took the principles of *Miller* and analogized them to the surveillance context, which solidified the foundation of the third-party doctrine and modern surveillance law.[140] The limited protections afforded to records kept by third parties from surveillance would be formally recognized in federal statute with the Pen/Trap provisions found in the 1983 Electronic Communications Privacy Act[141] ("ECPA").[142] The Pen/Trap provision provides a reduced standard for third-party records by requiring a court order through the ECPA or the Foreign Intelligence Surveillance Act of 1978[143] ("FISA").[144]

---

[137] *Id.* at 745; United States v. Miller, 425 U.S. 435, 442 (1976). An important component of the *Miller* decision was that the information supplied to the bank's staff needed to be viewed by the bank's staff in order to properly input the information, an aspect which is not necessary for the information at bar in *Smith*. *See id.* The recording of dialed numbers was entirely autonomous and would not be exposed to the telephone operators in the ordinary course of business. *See Smith*, 442 U.S. at 737.

[138] *Miller*, 425 U.S. at 442; *see generally* Hoffa v. United States, 385 U.S. 293 (1966); Lopez v. United States, 373 U.S. 427 (1963); Couch v. United States, 409 U.S. 322 (1973).

[139] *See* Smith v. Maryland, 442 U.S. 735, 743 (1979). The *Smith* Court believed that the majority of telephone users were aware that the telephone company recorded the numbers they dial. *Id.*

[140] *If These Walls Could Talk*, *supra* note 122, at 1929. The *Smith* Court created a more detailed analysis and clearer articulation of principles than the Court in *Miller*. *See id.*

[141] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508 §§ 3121-3126, 100 Stat. 1848, 1868-1873 (codified as amended at 18 U.S.C. §§ 3121-3127).

[142] 18 U.S.C. §§ 3121-3127.

[143] 18 U.S.C. § 3121(a).

[144] 50 U.S.C. § 1801. FISA presents its own Fourth Amendment problems in the wake of overbroad data collection by the NSA, which caused a major scandal after Edward Snowden disclosed government surveillance methods to the public. *See* James F. McHugh, *Book Review*, 97 MASS. L. REV. 19, 20 (2015) (reviewing GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014)). FISA provides a

III. Modern Surveillance Laws and the Digital Technology: What to Do?

The first and most obvious step in reforming the Fourth Amendment should be ending the third-party doctrine. Internet surveillance laws operate under the distinctions first established in *Jackson*, refined through *Smith.*[145] Without delving into an in-depth explanation of how digital technology functions, suffice it to say that the bevy of data obtainable from records held by third parties from digital technologies vastly exceeds the scope of that contemplated in *Smith* or *Miller.*[146]

A. Issues with the Third-Party Doctrine

The nature of how individuals interact with their devices has drastically shifted from the era of the landline telephone. Cell phones and computers are often essential for certain types of activities, careers, financial management, social media, dating, hobbies, entertainment, and expression.[147] Smart phone usage has exploded in popularity in the last decade, with eighty-one percent of Americans owning a smartphone in 2018, compared to thirty-five percent in 2011; nearly every American owns a cell phone of some kind, and almost every American younger than fifty owns a smart phone.[148]

---

warrant exception to foreign targets of surveillance, and even if that surveillance obtains communications from an American citizen, there still is no warrant requirement. Wadie E. Said, *Law Enforcement in the American Security State*, 2019 WIS. L. REV. 819, 841 (2019).

[145] *See* Bellovin et al., *supra* note 5, at 3-4.

[146] *Id.* See *id.* at 52-91 for a more technical and comprehensive demonstration of the complexities of internet architectures.

[147] By September of 2019, Apple's App Store had exceeded two million applications and generated more than $50 billion dollars in revenue in 2018 alone. Jack Nickas & Keith Collins, *How Apple's Apps Topped Rivals in the App Store It Controls*, N.Y. TIMES, (Sept. 9, 2019), https://www.nytimes.com/interactive/2019/09/09/technology/apple-app-store-competition.html [https://perma.cc/CUB7-S6XB].

[148] *Mobile Fact Sheet*, PEW RSCH. CTR., (Jun. 12, 2019), https://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/9P4J-SJWE]. Smartphone usage is least prevalent among individuals with an education level of less than a high school diploma and aged sixty-five or older. *Id.* Even among demographics least likely to have smartphones, ownership is above fifty percent for all demographics in America and has been trending upwards over the last decade. *Id.*

But even within the context of the relatively modest capabilities of the landline phone, the distinctions established by *Jackson*, the Wiretap Act, the ECPA, and *Smith* were ill-fitting.[149] By the 1980s, telephone companies began conveying more than simply dialing information and began storing bank accounts, user accounts, and prescription numbers.[150] Data sharing methods and data keeping by private corporations would only to continue to expand outward in volume, complexity, and the type from this point.[151]

Can the principles of *Jackson*, grounded in the realities of the late nineteenth century postal system, be adapted to digital technology? Legal scholars disagree.[152] Almost all scholars, however, recognize that the third-party doctrine at minimum needs to be rethought, if not abandoned in its entirety.[153]

Even the ECPA itself seems to disregard this concept with Title II, known as the Stored Communications Act ("SCA").[154] As the name implies, the SCA regulates the handling of stored electronic content such as e-mail, voicemail, and messages stored for over 180 days.[155] Electronic information that would otherwise enjoy Fourth Amendment

---

[149] *See* Bellovin et al., *supra* note 5, at 4 (noting that the competition offered by services competing with AT&T quickly altered the landscape of what was initially a relatively simple communication architecture).

[150] *Id.* Even at the time of *Smith*, companies were already utilizing more complex methods of landline communication that required the use of intermediaries to properly convey information needed for making certain types as calls, such as long-distance calls. *See id.*

[151] *See id.* at 5. IP-based communications, for example, rely on end-to-end communications, which are based in "dynamic" connections that depend on a wide range of underlying interworking networks in order to properly function. *Id*.

[152] *Accord id*; Tokson, *supra* note 43 (noting that there has been controversy of how traditional doctrine can be applied to digital technology).

[153] *Accord* Bellovin et al., *supra* note 5 (arguing for the abandonment of the doctrine); Tokson, *supra* note 43 (arguing for adding new factors to refine it). See Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009), for a discussion on why the third-party doctrine should be retained without alteration.

[154] Stored Communications Act (SCA) § 201, Pub. L. No. 99-508, 100 Stat. 1860, 1860-68 (1986) (codified as amended at 18 U.S.C. §§ 2701-2712).

[155] 18 U.S.C. § 2703(a). Records being seized under the SCA only require a court order which requires the government show "reasonable grounds to believe that the . . . records or other information . . . are relevant and material to an ongoing investigation." *Id.* § 2703(d).

protections and under normal circumstances require a warrant, only requires a subpoena or a court order if it has been stored for 180 days.[156]

The arguments for the abolition of the third-party doctrine from a privacy perspective are twofold. First, the design of internet architecture, massive amounts of data exchanged, and use of predictive analytics can allow government actors to discern or infer private, potentially sensitive data that should enjoy privacy protections when observing third-party records. For example, a webpage which displays the result of a user's search will transmit to a third party a URL that would allow a government actor to infer what the user was searching for.[157] Comparing third-party data records to a traditional letter, it would be as if the contents of the letter were written on the outside of an envelope.[158]

Second, third-party records may actually contain more sensitive and personal information than traditional communicative content itself.[159] Location data in particular has been the source of controversy, both in the Court with cases like *Jones*[160] and *Carpenter*[161] as well as in academia.[162] As Justice Sotomayor expresses with her concurrence in *Jones*, which Chief Justice Roberts cites favorably in *Carpenter*,

---

[156] *See* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 463-64 (2008). Cate highlights lower protection afforded to the stored communications under the SCA by comparing it to the relatively strong protections established under the Wiretap Act. Intercepting communications protected by the Wiretap Act requires a "super" search warrant which can only be sought be specially designated federal officials and has a litany of caveats to how the government intercept the communications and what information it can record. *Id.*

[157] Bellovin et al., *supra* note 5, at 70. For an example of how this specifically could apply to the field of predictive analytics, the retail outlet Target developed a system to predict when a woman was in the second trimester of her pregnancy by aggregating her shopping data. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?mtrref=www.google.com&gwh=4371066EA2F747005D100D0A1CA7636B&gwt=pay [https://perma.cc/BVD7-A5MG].

[158] *See* Bellovin et al., *supra* note 5, at 71.

[159] Neil M. Richards & Jonathan King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 393 (2014).

[160] *See* United States v. Jones, 565 U.S. 400 (2012) (regarding the collection of GPS data from a device attached to a suspect's car).

[161] *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).

[162] *See generally* Bellovin et al., *supra* note 5; Tokson, *supra* note 43.

location information can reveal intimate details about one's life, such as "familial, political, professional, religious, and sexual associations."[163]

The overly broad nature of the third-party doctrine compounds these issues, with many critics decrying the "binary" nature of privacy, the lack of real agency for the person handing over the information, and the lack of knowledge of how that information will be handled.[164] These critiques were first articulated by Justice Marshall and Justice Stewart in their dissents of *Smith* and have gained increased relevance as technology has developed in its capabilities.[165] In an article criticizing the dissipation of Fourth Amendment protections in the digital age, Daniel J. Solove, a professor at George Washington Law School, writes, "[w]e are becoming a society of records, and these records are not held by us, but by third parties."[166]

Professor Solove's words, written in 2002 and before the advent of the smart phone, have proven to be prophetic.[167] With internet technology, an end-user's information is often shared unknowingly, without his or her explicit consent.[168] Due to the profit model of many websites, applications, and services, such data collection is required by the end-

[163] *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).
[164] *See* Richards & King, *supra* note 159, at 396 (criticizing privacy as being treated similar to an "on-or-off" state); Bellovin et al., *supra* note 5, at 2.
[165] Smith v. Maryland, 442 U.S. 735, 748-52 (1979) (Marshall, J., dissenting); *id.* at 746-48 (Stewart, J., dissenting).
[166] Solove, *supra* note 9, at 1089. Solove further notes that "modern society demands" that individuals enter into a multiplicity of relationships that generate a multitude of personal records that are held by businesses. *Id.* The involuntary nature of this data collection required to participate in modern society would later influence the Court's opinion in *Carpenter*. *See Carpenter*, 138 S. Ct. at 2223.
[167] Solove, *supra* note 9, at 1089.
[168] *See* Richards & King, *supra* note 159, at 424. Richards further notes the dangers allowing continuous government into citizens' private domains as strengthen a government's ability to suppress speech and discriminate. *Id.*

user to use the platform.[169] In turn, the data collected is sold to or monitored by other corporations.[170]

Such arrangements, common as they are, impose serious difficulties for the continued practicality of the third-party doctrine in its current form. The expansive use of such doctrines allows government agencies such as the National Security Agency ("NSA") to garner an unprecedented amount of data without a warrant.[171] In 2018 alone, the NSA collected over 400 million call detail records from cell service providers, which is hardly the scale contemplated by *Miller* or *Smith.*[172]

From a property-based perspective, the third-party doctrine has generally enjoyed less criticism. Not because the advocates of the property-based perspective universally subscribe to the notions established by the third-party doctrine, but because criticism has been more squarely focused on the underlying *Katz* decision.[173] The

---

[169] *See id.* at 414. The exchange of information between companies is so widespread and so voluminous in nature that Facebook founder Mark Zuckerberg famously stated, "the age of privacy is over." *Id.* at 409; Marshall Kirkpatrick, *Facebook's Zuckerberg Says the Age of Privacy Is over*, READWRITEWEB (Jan. 10, 2010), https://archive.nytimes.com/www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html.

[170] Daniel Zwerdling, *Your Digital Trail: Private Company Access*, NPR, (Oct. 1, 2013, 2:00 PM), https://www.npr.org/sections/alltechconsidered/2013/10/01/227776072/your-digital-trail-private-company-access [https://perma.cc/XD69-PB4H]. For an example of how private corporations can obtain and sell potentially sensitive information about their users, dating applications, such as OKCupid, collect information about people's drinking habits, drug use, sexual habits, race, religion, and other details which in turn is monitored by advertising and research firms that curate an online profile based on the data garnered from OKCupid. *Id.*

[171] Cate, *supra* note 156, at 436.

[172] UNITED STATES OFF. OF THE DIRECTOR OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES 30 (2018), https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf.

[173] *See, e.g.*, United States v. Carpenter, 138 S. Ct. 2206, 2235 (2018) (Thomas, J. dissenting). Justice Thomas opines that the reasonable expectation of privacy test expressed in *Katz* was wrong, and the principal inquiry to discussed is whether data is the property is owned by the individual or the third party that maintains it. *Id.* Justice Thomas concludes the analysis by stating that data is owned by the third party, not the individual being searched, therefore the data is not protected by the Fourth Amendment. *Id.; see also id.* at 2247 (Alito, J., dissenting) (conducting a similar analysis to Justice Thomas). Justice Alito, while preferring a property-based perspective, seems to more willing to retain *Katz*, as he does not explicitly disapprove of its use and is willing to conduct a *Katz* analysis as long as it falls within the limits of the property-based perspective; he criticizes it as "broadening the [Fourth] Amendment's reach." *See id.*

traditional property-based perspective does not evaluate the privacy expectations of the individual—instead, it is only concerned with the object being seized and to whom it belongs.[174]

Functionally, the third-party doctrine achieves the same result as the traditional property-based analysis, albeit for differing reasons.[175] However, in recent years, a new understanding of the property-based perspective has emerged. The new property-based perspective could integrate the privacy and property-based perspectives, but also extends Fourth Amendment protections to digital technology as well.[176]

B. Can *Carpenter* Change Everything?

The recent *Carpenter* case involved the Court's latest effort to tackle the issues regarding the third-party doctrine. While *Carpenter* represents a step in the right direction, the Court has not gone far enough in fully abrogating the third-party doctrine. Nonetheless, *Carpenter* proves instructive in demonstrating the difficulties in creating a Fourth Amendment standard for digital data.

Timothy Carpenter had been named as an accomplice in a series of armed robberies of Radio Shack and T-Mobile stores in Michigan and Ohio by one of the perpetrators, who turned Carpenter's cell phone

---

[174] *See id* (Alito, J., dissenting). Justice Alito also places comparatively more weight on the distinction between an "order" and a "search" than the other two property-based Justices. *See id.* In Justice Alito's words, an order only requires a party to look through its own records and provide a document, whereas a search involves the dispatching of law enforcement to enter private premises to seize private effects; an order does not invoke the Fourth Amendment at all, whereas a search does. *Id*.

[175] From the perspective of the third-party doctrine, the Fourth Amendment does not apply because it the individual being searched has a reduced privacy interest in the third-party records because they are held by a third party. From the traditional property-based perspective, the Fourth Amendment does not apply because the data being searched by the government belongs to third party; expectation of privacy is not a relevant interest. The result is the same regardless of which perspective: the data does not enjoy Fourth Amendment protections.

[176] *See Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J. dissenting). Breaking from his peers, Justice Gorsuch states that certain property interests may be found in digital data that is held by third parties through the concept of bailment and suggests categorizing such data as part of one's "effects" under the Fourth Amendment. *Id.* Further, Justice Gorsuch asserts that people have "substantial legal interests" in their digital data. *Id.* at 2272.

number over to the FBI.[177] The FBI applied for court orders under the SCA to obtain the call records of Carpenter, seeking 152 days of CSLI from MetroPCS as well as seven days from Sprint.[178] The data confirmed that Carpenter's phone was at the location of the four robberies at the same time and the same day as the robbery occurred.[179] On the basis of this evidence, Carpenter was convicted and sentenced to over 100 years in prison.[180] Carpenter appealed on Fourth Amendment grounds because the CSLI had been obtained without a warrant supported by probable cause.[181]

The Court agreed.[182] Justice Roberts, writing for the majority, stated that given the revealing and automatic nature of CSLI data collection, the acquisition of the data was a search under the Fourth Amendment.[183] The ruling was narrowly tailored, with Justice Roberts explicitly stating that the ruling only applied to the context of CSLI—*Smith* and *Miller* were not be disturbed, and the rule was not intended to question conventional surveillance techniques or tools.[184] Nonetheless, there has been a debate on how "narrow" this narrow decision is in reality.[185]

Much of Robert's opinion is dedicated to how the circumstances of CSLI tracking qualitatively differ from the phone records and banking information seized in *Smith* and *Miller*.[186] The Court, invoking *Katz* and Justice Sotomayor's concurrence from *Jones*, states that an individual

---

[177] *Id.* at 2212 (majority opinion).
[178] *Id.*
[179] *Id.*
[180] *Id.* at 2213.
[181] *Id.*
[182] *Id.* at 2223.
[183] *Id.* However, Justice Roberts acknowledges that this is not a categorical warrant requirement for the search of CSLI and known exceptions to warrant requirements, such as the exigent circumstances exception, still apply. *Id.* at 2222.
[184] *Id.* at 2220. Justice Roberts further notes that warrants will only be required in the "rare case" where the suspect has a legitimate privacy interest in the third-party records. *Id.* at 2222.
[185] *See, e.g.*, Kyllie Mae Guidry, Carpenter v. United States: *A Step Further in Privacy Protection, but Not Far Enough*, 46 S. UNIV. L. REV. 260 (2019); Ohm, *supra* note 19; Burrus & Knight, *supra* note 19; Mezera, *supra* note 19. The general impression of most academics is that *Carpenter* has significantly affected the future applicability of the third-party doctrine, despite being characterized as a "narrow" holding. *See, e.g.*, Ohm, *supra* note 19.
[186] *Carpenter*, 138 S. Ct. at 2217-19. Justice Roberts is particularly concerned about the differences between the nature of the data collected in aggregate. *See id.*

has a reasonable expectation of privacy as to his or her physical location.[187] Invoking *Miller* and *Smith*, Justice Roberts argued that Carpenter did not share his information voluntarily, as cell phone use is essentially a necessity in today's society that could not in any meaningful way "assume the risk" of turning over CSLI to third parties.[188] Additionally, the Court noted that the third-party doctrine did not anticipate the "world of difference between the limited types of personal information . . . and the exhaustive chronicle of location information casually collected by wireless carriers today."[189] From Robert's perspective, using the third-party doctrine to obtain information such as CSLI would be impermissibly extending the scope of the third-party doctrine outside its intended function.[190] But does that logic hold water?

C. The New *Carpenter* Test?

Despite Robert's repeated insistence to the contrary, *Carpenter* significantly alters the third-party doctrine and the interpretation of *Smith* and *Miller*.[191] The logic underlying the decision in *Carpenter* can easily be transposed to other emerging technologies which present novel methods of undermining privacy. Some commenters have gone as far as to say that *Carpenter* implicitly creates an entirely new test.[192]

Paul Ohm, a professor at Georgetown University, notes that the critical factors of the *Carpenter* analysis include the (1) "deeply revealing nature" of the information; (2) its breadth, depth, and comprehensive reach, and (3) the automated and unescapable collection of data.[193] Ohm posits that when lower courts attempt to apply this new "test" established under *Carpenter*, many databases that have never required a warrant will now be covered under the Fourth Amendment.[194]

---

[187] *Id.* at 2218.
[188] *Id.* at 2220.
[189] *Id.* at 2219.
[190] *Id.*
[191] Ohm, *supra* note 19, at 358.
[192] *Id.* at 361.
[193] *Id.*
[194] *Id.*

Ohm characterizes the rejection by Chief Justice Roberts to use existing precedent as "tech exceptionalism," which stands for the premise that advances in information technology create novel circumstances that have not been addressed by existing precedent and attempting to analogize previous precedent with new technology is inappropriate.[195] For example, "tech exceptionalism" would reject the idea that a pen register can be directly compared to a telephone operator, as the Court did in *Smith.*[196]

This approach, while on its face is seemingly a practical escape route for the Court, has several problems—the first and foremost being that it provides no real guidance to ensure consistency in future cases. Consequently, the approach will lead to inconsistent results and applications. While *Carpenter* admits that there are exceptions to the third-party doctrine, it does not provide any sort of method to categorize or define those exceptions. Justice Roberts merely calls it a "different species of business records."[197] Instead of using the paradigm of communicative content versus records held by third parties, the Court now suggests there may be a third category of information that lacks any definite meaning. Moreover, it does nothing to prevent the lower courts from acrimoniously applying the rule from *Smith* to new technology; it only gives them the option to elect to disregard *Smith* if they so choose. Yet, the possibility to remedy this shortcoming may be found in the most unlikely of places: the property-based perspective.

IV. The Future of the Fourth Amendment

Carpenter remains an incomplete solution to deal with Fourth Amendment treatment of digital data. While some commenters have considered *Carpenter* to be a revolutionary expansion of the Fourth Amendment, it has left others unsatisfied both from a doctrinal consistency and privacy perspective.[198] Those who have been left cold

---

[195] *Id.* at 360.
[196] Smith v. Maryland, 442 U.S. 735, 745 (1979).
[197] Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).
[198] *See* Guidry, *supra* note 185; Burrus & Knight, *supra* note 19. Among the chief criticisms of *Carpenter* is that the framework does not do enough properly advocate privacy interests (from the perspective of privacy advocates) and does not provide a sufficient or principled

by *Carpenter* have turned to Justice Gorsuch's dissent,[199] which calls for the abandonment of the reasonable expectation of privacy test from *Katz* and expansively redefines the property perspective to be digital data inclusive.[200] Combining Gorsuch's expansive property perspective with the new *Carpenter* privacy perspective may resolve the numerous problems with digital data and the Fourth Amendment.

Justice Gorsuch proposed that the legal concept of bailment be used to address the issue of third-parties and digital data.[201] Invoking *Jackson*, Justice Gorsuch argued that digital data are the modern equivalent of "papers and effects" entrusted to a third party.[202] A bailee owes a legal duty to keep an item safe for the bailor; Justice Gorsuch claims that this can be analogized modern data keeping.[203] By considering data as one's "papers and effects," the Fourth Amendment interest can be maintained even if it is given to a third party.[204]

---

framework to enumerating Fourth Amendment rights based in the language of the Amendment (from the property-based perspective). *Id.* Justice Gorsuch specifically critiques the holding in *Carpenter* as creating "two amorphous balancing tests, a series of weighty and incommensurable principles to consider in them, and few illustrative examples that seem little more than the product of judicial intuition." *Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J., dissenting).

[199] Burrus & Knight, *supra* note 19, at 82. Although Justice Gorsuch's dissent was not joined by any of the other dissenting Justices (Thomas, Kennedy, or Alito), his perspective on the property based Fourth Amendment has gained traction with certain academics who advocate for that perspective. *See generally id.*; *Carpenter*, 138 S. Ct. 2206.

[200] *Carpenter*, 138 S. Ct. at 2268-70 (Gorsuch, J., dissenting). Justice Gorsuch's main critique of *Katz* comes from its "often unpredictable—and sometimes unbelievable—jurisprudence." *Id.* at 2266.

[201] Burrus & Knight, *supra* note 19, at 97. Worth noting, however, is Justice Gorsuch's apparent willingness to retain *Katz* to some degree, as he admits in *Carpenter* that there are "some occasions where *Katz* is capable of a principled application." *Carpenter*, 138 S. Ct. at 2265 (Gorsuch, J., dissenting). Justice Gorsuch further suggests that a "principled application" of *Katz* would result in the same conclusion as a "more traditional option." *Id.* at 2266.

[202] *Carpenter*, 138 S. Ct. at 2269 (Gorsuch, J., dissenting).

[203] *Id.* at 2269-71. Justice Gorsuch does not express a definitive opinion on if there is a proprietary interest metadata generated in response to user "lending" of information, or how many steps removed from a particular user input could potentially terminate a user's property interest.

[204] *Id*. Justice Gorsuch highlights that complete ownership or exclusive property control is not a necessary condition to enjoy a Fourth Amendment right. *See id.* at 2269. For example, tenants that reside in a rental property still enjoy Fourth Amendment protection of their living area even though they do not own the property itself. *Id.* at 2269-70.

The European Union has done something similar with its General Data Protection Regulation ("GDPR").[205] The legislation is intended to protect the rights of consumers by affording them a limited ownership and set of rights to their data collected by third parties.[206] The need for the GDPR reflects the chicken or the egg problem that results from the creation and categorization of new technology: Does the legislation exist because the end-user *already has* property interests in their digital data and therefore needs to be protected as such, or does the GDPR *create* a new, statutorily defined expansion of property interests? For Justice Gorsuch, the answer is the former.

Should the Fourth Amendment head toward solely a property regime? The drawbacks to the property analogy have already been expressed by Ohm with the concept of "tech exceptionalism."[207] Analogizing old principles to new and novel technology leads to the decisions such as *Smith*, so if the goal is preventing another *Smith*, Justice Gorsuch's suggestion to treat data as analogous to bailment has similar shortcomings.[208] Additionally, the property-based standard still has the shortcomings of *Katz* that it purports to solve, which are ambiguity in differentiating between different species of property and deciding on a coherent calculus that balances the individual's right to their "papers and effects" against legitimate government inquiry.

---

[205] Commission Regulation 2016/679, 2016 O.J. (L 119) [hereinafter GDPR]. The GDPR provides several restrictions on the handling of data between public and private entities, as well as violations for noncompliance. *See id.*

[206] *See* Jacob M. Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513 (2013). Most notably, the GDPR attempts to establish a "right to be forgotten" that entitles an end user to order the deletion of records held by third parties that contain that end user's data. *Id.* at 513-14. However, this "right to be forgotten" does not merely extend to the third party that creates or keeps the records, but *all* third parties with whom the information has been shared or sold. *Id.* at 514.

[207] Ohm, *supra* note 19, at 360, 400-02. Ohm speculates that lawyers and legal scholars in particular are vulnerable to making erroneous conclusions based on analogies because they are "non-experts who cannot understand the failure of a given analogy because they cannot accurately characterize Y or compare it to X when complicated analogy in involved." *Id.* at 407. To accommodate for this shortcoming, Ohm suggests employing "sophisticated technological support" and emphasizes the need for interdisciplinary training. *Id.*

[208] *See id.* at 406-08. In particular, Ohm highlights that technology such as the smart phone have no historical analogy and speculates that Justice Roberts considers the contents of a smart phone to have a stronger privacy interest than the traditionally protected home. *Id.* at 403.

Alone, the concept of bailment applied to digital property provides only limited use. But reading Justice Gorsuch's dissent as a critique of the current *Katz* standard demonstrates a potential compromise between a privacy-based "tech exceptionalism" and Justice Gorsuch's desire for a stronger Fourth Amendment based in property-principles. While the privacy and property-based perspectives differ on the methodology, proponents of both the Gorsuch property perspective and privacy advocates agree on not only the problem, but also the result: *Katz* and *Smith* create too many issues.[209] Further, and perhaps even more importantly, they agree Fourth Amendment protections need to include digital data and that current measures are inadequate.[210] The unification of goals and common grievances make a bipartisan Fourth Amendment possible.

A. "Public-Facing" Data and Presumption of "Tech Exceptionalism"

The problem inherent in both Roberts's "tech exceptionalism" and Justice Gorsuch's property-based standard is that both doctrines fail to adequately account for unexpected societal changes associated with the development of new technology. Roberts's tech exceptionalism is a purely reactive set of limitations to an overly exclusive doctrine and still too amorphous and unclear for practical use,[211] while Justice Gorsuch's

---

[209] *Compare id.* at 416 (stating the Fourth Amendment has failed to properly account for the harms that can be wrought with new technology), *with Carpenter*, 138 S. Ct. at 2261-62, 2272 (Gorsuch, J., dissenting) (criticizing current precedent as "doing nothing to limit investigators from searching your records you've entrusted to your bank, accountant, and maybe even your doctor" and suggesting that a constitutional floor may be necessary to bar efforts to circumvent Fourth Amendment protections with a subpoena).

[210] *Compare* Bellovin et al., *supra* note 5 at 91-92 (criticizing *Katz* and *Smith* as being too difficult to apply and leading to inconsistent and anomalous results), *with Carpenter*, 138 S. Ct. at 2266 (Gorsuch, J., dissenting) (leveling the exact same criticism of *Katz* and *Smith*).

[211] Although Ohm advocates for a more expert-integrated approach concurrent with "tech exceptionalism," it is important to consider the current reality of the legal system with regards to the technological literacy of most judges and magistrates approving court orders, a fact highlighted by Justice Gorsuch in his dissent in *Carpenter*. *See Carpenter*, 138 S. Ct. at 2265 (Gorsuch, J., dissenting) (stating that Federal judges are often ill-equipped to make such decisions). Important to consider is the fact that the average age of an Article III Judge is around sixty-five years and continues to increase every year. *See* FED. JUDICIAL CTR., *Demography of Article III Judges, 1789-2017*, https://www.fjc.gov/history/exhibits/graphs-and-maps/age-and-experience-judges#_ftn7 [https://perma.cc/DS9H-8WE4]. Consequently, it

property-based standard fails to grasp the multitude of relationships an individual can have with their data.[212]

For an illustration of both doctrines' respective shortcomings, one would only need to look at how applications function in the modern world. A person in today's society may knowingly and voluntarily tender location information to the dating app Tinder[213] but nonetheless be perturbed by the notion that the government can seamlessly access and aggregate that information without a warrant.[214] Similarly, it would be hard to argue that the association created by a Tinder "match" could be conceived as property or having a property interest in a straightforward, traditional manner, but it would generally be considered invasive for the government to monitor who matches with whom.

In both above hypotheticals, the expectation of privacy should be broken by the government intruding in a sphere where the information in question would not be available to another end-user of the platform. Put differently, the data is not "public-facing." Tinder users cannot view the matches of other Tinder users nor track each other's exact locations.[215]

---

is desirable to have clearly defined rules or principles that make it easier for a judge that may not have a strong background in technology to make a decision, and not merely defer to the opinion of an expert.

[212] Justice Gorsuch's perspective is problematic when applied to the concept of predictive analytics or third-party records generated in response to or from user input data. For example, if a company compiles a user's data and assigns labels to certain users based on a set criterion, would the user have any property interest in that record if the company's categorization would reveal the underlying data it used to make a judgment? Retaining the *Katz/Carpenter* privacy principles allows for malleability in fringe cases and for unpredictable advances in technological development that may not be covered under the bailment concept.

[213] Given the volatile nature of technological progress, applications like Tinder may become out of date, unsupported, or otherwise no longer used in the near future. The use of examples in this Note are intended to illustrate clearly articulable principles for classifying and analyzing various species of data moving into the future without limiting the analysis to the current technological paradigm or existing platforms.

[214] *See generally Carpenter*, 138 S. Ct. 2206 (finding a reasonable expectation of privacy exists for location data given to a third party for that third party's use, but only if that data is collected automatically without one's knowledge).

[215] Marie Black, *How to Use Tinder*, TECH ADVISOR, (Apr. 29, 2019) https://www.techadvisor.co.uk/feature/software/tinder-3515013/ [https://perma.cc/5DC2-8397].

Tinder sells that information to other corporations as part of its profit model, but that data is not publicly available.[216]

Under the *Katz* reasonable expectation of privacy test, the end-user and society *should* have a privacy expectation regarding data not viewable by the public because for all intents and purposes, the data is not seen or expected to be seen by anyone.[217] However, *Katz* has not been historically applied in that manner.[218]

By contrast, a Tinder user may expect that his or her profile pictures, description, and general whereabouts may be ascertained by other users, as the end-user deliberately places that information in a place where it can be viewed. The purpose of the data is to be seen by others. Put another way, those types of data are "public-facing."

The concept of "public-facing" data is as old as *Jackson* itself. When Jackson sent his lottery flier that could be viewed by anyone without any additional inspection, he forfeited his Fourth Amendment interest in the secrecy of the contents of his flier.[219] The Court characterized this

---

[216] Judith Duportail, *I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets*, GUARDIAN, (Sept. 26, 2017, 2:10 AM), https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold [https://perma.cc/BV7B-NFVT]. The types of data Tinder has stored behind closed doors include: every location where a message is sent from with timestamps, age range of partners, education level of the user, occupation, and tastes in food. *Id.* In Europe, the data compiled by Tinder is statutorily required to be accessible to the end user when requested, but no such mechanism exists in the United States. *Id.*

[217] Justice Marshall suggests that this is the proper formulation of the *Katz* inquiry in his dissent in *Smith*.
Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting). Justice Marshall further criticizes the idea that professional or personal necessities such as phone calls requires the "assuming" of risk of surveillance. *Id.* at 750.

[218] *See id.* One of the primary critiques of *Katz* from both advocates of the privacy and property-based perspective is the inconsistency in its application. *See generally*, Bellovin et al., *supra* note 5; Burrus & Knight, *supra* note 19. For a discussion on how the concept of "knowing exposure" has been evaluated under the *Katz* framework, see Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of Remedy*, 55 STAN. L. REV. 119 (2002) (discussing the doctrinal flaws of the Fourth Amendment in a variety of circumstances including trash collection, flights, and tracking devices).

[219] *Ex parte* Jackson, 96 U.S.727, 733 (1877). By contrast, if Jackson had decided to conceal the contents of his letter with an envelope, thus keeping it safe from public inspection, the government would have had to obtain a warrant to inspect it. *See id.* The primary principle

as the "outward weight and form" in *Jackson.*[220] The same principles can be applied to modern data collection by the government.

B. Tipping the Scale in Favor of the Protection

Instead of the Court's broad approach to allowing government collection of data except that what is exceptional—such as CSLI—the paradigm should be reversed. The prevailing presumption should disallow the collection of data except that which can be safely described as having minimal privacy interests.[221] In other words, the Fourth Amendment should safeguard people's information as long as it is not "public-facing." What constitutes "public-facing" in the digital technology context is data that can be openly and easily accessed by an ordinary end-user or information put on public display for the purposes of others' use on the platform.

This paradigm can be justified under Justice Gorsuch's property perspective as well. Information that is given to a third party for the purpose of public display creates a distinctive property relationship between the two parties that can be separated from information that is provided for the purposes of record keeping or required to operate the platform.[222] Essentially, the "effects" in question given to the third party

---

expressed by *Jackson* is that the government need not blind itself to something that is on public display merely because it is another person's "papers" under the Fourth Amendment. *See id.*

[220] *Id.* The wording of "outward weight and form" is meant to indicate the physical appearance and weight of the parcel easily observed without inspection. *See id.*

[221] In other words, data meant for public consumption or that is otherwise easily publicly viewable. This integrates the privacy principle Justice Marshall expressed in *Smith* and analogizes it to the digital sphere. *See Smith*, 442 U.S. at 749.

[222] *See* Carpenter v. United States, 138 S. Ct. 2206, 2268-70 (Gorsuch, J., dissenting). Justice Gorsuch uses an analogy comparing an intrusion of a tenant or resident family members who technically do not own the property to digital data to illustrate that merely because the individual does not have a legal title or ownership to the property, it does not eliminate their Fourth Amendment interests. *Id.* However, "public facing" data can be contrasted with record data on two grounds: (1) the purpose for which the data is being conveyed and (2) who the recipient of the data is. Essentially, the data in question that is "public facing" can be considered data that is given to the public at large and therefore terminates the proprietary interest of the information, whereas record data is a bailment provided to a company in exchange to use a service. The analysis is intended to avoid creating complex normative questions for the Court to decide regarding the subjective expectations of the end user and discourage the use of analogies.

are *meant to be used and consumed by the public*, much like how one takes out an advertisement on a billboard. The third party in this situation is merely the middleman to provide the individual's "effects" to the public. By contrast, data that is provided to a bailor as a condition to access a platform, or otherwise for the purposes of utilizing some sort of service retains the traditional bailee-bailor relationship wherein the bailee's interest in the property remains.[223]

It is clear that the third-party doctrine as defined under *Smith* and *Miller* is buckling under the weight of its own impracticality and the restrictions set forth by *Carpenter*.[224] The act of surrendering certain information to a third party should not terminate an individual's privacy or property interest in that information. While there are some instances where a privacy or property interest can terminate through voluntarily and explicitly surrendering the information to third parties with the knowledge that it will be viewed by others, as in *Miller* and *Jackson*, the vast majority of data turned over to third parties do not share those clear-cut circumstances.[225] As Justice Marshall wrote in his dissent of *Smith*, privacy should not be treated like an on/off switch.[226]

Consequently, the new paradigm should be predictive rather than reactive. Justice Brandeis was rightfully concerned about technology's ability to undermine the Fourth Amendment interests of the individual in his *Olmstead* dissent, but the Court has not crafted any safeguards to anticipate this. As seen in *Carpenter*, the issue becomes that the

---

[223] *Id.* (Gorsuch, J., dissenting). Justice Gorsuch also notes that data required to operate technology which is "functionally compelled by the demands of modern life" may be considered to be a type of "involuntary bailment." *Id.* Justice Gorsuch's concerns echo Justice Marshall's original critique of *Smith*. *See Smith*, 442 U.S. at 749-50 (Marshall, J., dissenting) (expressing skepticism that people realistically have a choice when "choosing" to use telephone technology).

[224] *See generally* Ohm, *supra* note 19; *Carpenter*, 138 S. Ct. at 2261-70 (Gorsuch, J., dissenting). Despite being supposedly on opposite ends of an ideological spectrum, both Ohm and Justice Gorsuch share the same critiques of *Smith* and *Katz*. *Compare* Ohm, *supra* note 19, *with Carpenter*, 138 S. Ct. at 2261-70 (Gorsuch, J., dissenting).

[225] *See generally* Richards
& King, *supra* note 159. The vast majority of information collected about a user in the digital sphere is done so without the user's explicit knowledge or consent. *Id.*

[226] *Smith*, 442 U.S. at 749 (Marshall, J., dissenting). Justice Marshall posits that privacy should follow more of a spectrum, as certain species of data can be more or less sensitive than others. *Id.*

government can collect any information or use any means that it is not explicitly forbidden from using.[227] This is not a desirable outcome.[228]

The scales need to be tipped in favor of the individual, as opposed to the government. To update the Fourth Amendment, the Court needs to recognize this fact, disregard the third-party doctrine as it applies to digital data, and create precedent that allows for a presumption that favors the individual over the government.[229] The concept of "public-facing" data allows for such a protection. By creating a clearer and stricter standard of scrutiny for government surveillance, the Court would head off problems of emerging technology circumventing Fourth Amendment protections through increasingly creative data collection and aggregation methods.[230] Only through anticipatory—not reactionary—doctrines can the Court protect the Fourth Amendment rights of Americans in the digital age.

C. The Bipartisan Fourth Amendment: Combining Property and Privacy Perspectives

The current status of the Fourth Amendment remains in flux. The lack of tangible and easily understood principles expressed in *Carpenter* creates difficulties for conducting a meaningful Fourth Amendment analysis in the realm of digital technology. Consequently, the rulings by the lower courts will tend to vary in scope and result until a clearer

---

[227] *See generally Carpenter*, 138 S. Ct. at 2206.

[228] For an in-depth discussion on the consequences of unregulated government data mining, see Cate, *supra* note 152 (highlighting the lack of statutory protection and a general unwillingness for the government to engage in self-regulation of its own surveillance activities).

[229] A possible method for facilitating this would be eliminating the presumption of reduced privacy interest in data held by third parties and instead invoking a rebuttal presumption of data protection. Creating a rebuttal presumption would combat a judge's willingness to defer to government's experts and request, instead requiring the judge to critically evaluating the principles at stake before allowing a surveillance order.

[230] Another potential benefit would be giving the lower courts a clear directive and avoiding complicated inquiries into the precise functionality of any particular application. As noted before and expressed by Justice Gorsuch, courts generally are not adept at making judgments on technological privacy issues. *See Carpenter*, 138 S. Ct. at 2265 (Gorsuch, J., dissenting) ("[P]olitically insulated judges come armed only with attorneys' briefs, a few law clerks, and their own idiosyncratic experiences . . . hardly the representative group you'd expect (or want) making empirical judgments for hundreds of millions of people.").

analysis can be articulated. Nonetheless, there is a general agreement among a majority of the Court that digital data deserves Fourth Amendment protections, but disagreements about how the doctrines should be handled.[231] Integrating aspects from Justice Gorsuch's property-based perspective into the reasonable expectation of privacy test may alleviate these issues.

Accepting Justice Gorsuch's conclusion that end-users have still retained property interests in their digital data shared or generated by third parties, digital data should be presumed to be protectable. The user's Fourth Amendment interests do not terminate merely because it is given to a third party, as the user still retains a proprietary interest in it. As many Justices supporting the property-based perspective have noted, *Katz* did not abridge the blanket Fourth Amendment protection to a person's papers and effects.[232] Nonetheless, the *Katz* analysis, particularly under *Smith* and *Miller* has moved away from this constitutional "floor" for protection and often cuts against it.

The focus of a combined privacy-property analysis should be: For what purpose is the user's data being "lent" to the third party? Are the data collected necessary to use the platform in question are they placed on display for the public ("public facing")? The strength of the property (i.e., the extent to which the records in question can be characterized as a person's "effects") and privacy interest (i.e., the extent to which a person expects that property to be "private") should inform whether the reasonable expectation of privacy exists.

For an example of how this combined analysis could work, consider again the example of Tinder. To use Tinder, an end-user must input their dating preferences by swiping right or left on other end-users'

---

[231] *Id.* Justice Gorsuch's dissent in Carpenter can be read as functionally similar to a concurrence rather than a dissent, because he appears to agree with the result achieved by the Court, but not the methodology.

[232] *See, e.g.*, United States v. Jones, 565 U.S. 400, 947 (2012) (noting that *"Katz* did not repudiate the understanding that the Fourth Amendment embodies a particular concern for government trespass upon the areas it enumerates"); Carpenter v. United States, 138 S. Ct. 2206, 2267 (2018) (Gorsuch, J., dissenting).

profiles.[233] In essence, the "effect" being supplied to Tinder by swiping is the information the user provides about his or her dating preferences; Tinder merely acts as a middleman to allow the user to match with another end-user.[234]

Since there is an "effect" being supplied to Tinder in the form of tangible data, the constitutional posture for the Fourth Amendment should favor protection. But the inquiry need not stop there. The follow-up should be: What is the function of the bailment? Is the purpose of the "effect" being supplied to be viewed by the public?

In the case of Tinder swipes, the answer would be no. Tinder does not alert the public at large about an individual's swiping habits.[235] The only time an end-user's swipe is revealed is either through a "super like" which indicates to a specific user that he or she has "super-liked" them in order to increase his or her profile visibility to that specific user, or when two users have independently swiped to match with one another.[236] Given the limited purpose for which the information was "lent" to Tinder, and the limited dissemination of the information in question, the contents of one's Tinder swiping habits should enjoy Fourth Amendment protections.[237]

---

[233] Marie Black, *How to Use Tinder*, TECH ADVISOR, (Apr. 29, 2019) https://www.techadvisor.co.uk/feature/software/tinder-3515013/ [https://perma.cc/CHN6-T5EN].

[234] *Id.* Tinder also has an opt-in algorithm to help a user assess profile favorability to better facilitate the matching process, which can dictate how a user's information is displayed on their profile without consulting the user, as well as other features that otherwise provide automated assistance in assisting profile visibility. *Id.* For the purposes of this analysis, however, bonus opt-in features such as paid subscriptions or methods to boost profile visibility will not be discussed.

[235] *Id.* Tinder, however, does keep records of this information to better generate possible matching profiles for individuals that use the platform. *Id.*

[236] *Id.* Even so though the information of a "match" or "super-like" is transmitted to another user, it is not handed out to the public at large. *See id.*

[237] For a more complex illustration of the same principles at work, consider the issue of location data with regards to Tinder. In order to use the platform, Tinder requires the use of location data, and that data is displayed publicly for other users to evaluate their location relative to the profile they are viewing. Such data, despite being one's effects, would not enjoy Fourth Amendment protections, as it is publicly viewable and carries with it no expectation of privacy. There is a reduced property interest as well, as the user voluntarily surrenders that "effect" to the public at large. However, precise location data of the user generated over a long

V. Conclusion

By integrating the notions of Justice Gorsuch's broader property-based regime into the *Carpenter* privacy-oriented extension of the *Katz* test, the test can become less opaque, easier to apply, and more objective. Additionally, it furthers the goals of privacy advocates by providing a blanket protection that must be overcome in order to protect new species of data, rather than asking a normative question of how society at large tends to view such data (a function that most courts are ill-equipped to accomplish). This would prevent the Court from having to decide a purely normative question to determine whether each and every new technology deserves privacy protection.

In a sense, everyone wins: those who have a property-based perspective of the Fourth Amendment have their preferred ideological framework as the baseline for the Fourth Amendment, and those with the *Katz* perspective are able to retain a flexible, privacy-oriented test.

Allowing for a more "principled" application of *Katz* and *Carpenter* would diminish potential critiques stating that its basis is not found in the Fourth Amendment. Additionally, it would eliminate the lower courts from reaching abnormal, unexpected results that arise from the application of *Katz*.[238]

The solution will not work for everyone, however. More originalist Justices such as Thomas or Alito likely will resist the categorization of digital data as property and maintain their stated positions as expressed in *Carpenter*. Nonetheless, the involvement of such Justices is not required to achieve a solid intellectual majority on the Court,[239] and it is

---

period of time, which would otherwise be unavailable for consumption to a typical Tinder end-user, likely would enjoy Fourth Amendment protections.

[238] Operating under the assumption that *Carpenter* creates a new test, the integrated *Katz/Carpenter* test would retain the same benefits.

[239] With Justice Gorsuch's vote, the Court could form a strong five-person coalition of Justices Roberts, Breyer, Kagan, and Sotomayor. While it is not currently known what Justice Kavanaugh or Barrett's opinion will be on these issues, the effort to craft an ideologically bipartisan Fourth Amendment may be enough to garner their vote as well, making the total 7-2.

apparent based on their prior rulings that they will not be convinced to adopt a more data protective Fourth Amendment.[240]

A synthesis between the property-based perspective and the privacy perspective would not only have the effect of improving the *Katz* test, but actively protect data interests. Further, it would allow for a bipartisan recognition of principles and ideals, which would be desirable for continued doctrinal consistency of Fourth Amendment jurisprudence moving forward.

[240] *See generally* United States v. Carpenter, 138 S. Ct. 2206 (2018) (Justices Alito and Thomas refusing to categorize data as a person's "effects" for a Fourth Amendment analysis). Justice Alito in particular gave a scathing critique of the majority's holding in *Carpenter*, predicting that the Court will face "embarrassment" of explaining a "crazy quilt of the Fourth Amendment." *Id.* at 2261 (Alito, J., dissenting).